Notice of Allowability	Application No.	Applicant(s)	
	10/082,385	PABLA ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12 June 2006*.

2. ☒ The allowed claim(s) is/are *1-65*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 27 March 2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 56-65 have been amended.

2. Claims 1-65 are pending.

Information Disclosure Statement

3. The Information Disclosure Statement respectfully submitted on 27 March 2006 has been considered by the Examiner.

Response to Arguments

4. Applicant's arguments filed on 12 June 2006 have been fully considered and they are persuasive.

Allowable Subject Matter

5. **Claims 1-65** are allowed.

6. The following is an examiner's statement of reasons for allowance: The present invention is directed towards a method and system for exchanging secure messages and other data between peers in a peer-to-peer environment. Claims 1,15,33,45, and 56 identify the uniquely distinct feature "**the second peer generating a first session key from the first public key**". Claims 25 and 29 identifies the uniquely distinct features "**generating one or more session keys from one or more public keys of the plurality of peers**". The closest prior art, Huitema et al. (Pub No. 2003/0056093) discloses a method for ensuring valid and secure peer-to-peer communications in a group structure, wherein the Owner invites an individual peer to join a group, generates a key to be used when communicating between group members, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious. The

closest prior art, Klonowski (US Patent No. 5,479,514) discloses a secure network data communication technique that allows the designation of selected network nodes to share encryption keys with other selected network nodes, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious. The closest prior art, Faccin et al. (Pub No. 2002/0118674) discloses a method and apparatus are provided for exchanging Diffie Hellman keys, however Faccin et al. fails to disclose a method for generating session keys from the public (Diffie Hellman) keys, therefore, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious. The closest prior art, Jablon (US Patent No. 7,010,692) discloses a method for two parties (Alice and Bob) to use a small shared secret (S) to mutually authenticate one another other over an insecure network by using separate public (Diffie Hellman) keys, however, Jablon fails to disclose sending one public key from the first peer to the second peer and the second peer generating the first session key from the first public key, therefore, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious.

7. Therefore, **claims 1,15,25,29,33,45, and 56** and the respective **dependent claims 2-14,16-24,6-28,30-32,34-44,46-55, and 57-65** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
June 22, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER